# AN ENHANCED ATTRIBUTE-BASED PRETTY GOOD PRIVACY FILE ENCRYPTION FOR DATA SECURITY IN ELECTRONIC MEDICAL RECORDS

**EDOSOMWAN, IMUETINYAN BOMA**
**(11CH012188)**
**B. Sc Management Information System, Covenant University, Ota.**

**OCTOBER, 2020**

# AN ENHANCED ATTRIBUTE-BASED PRETTY GOOD PRIVACY FILE ENCRYPTION FOR DATA SECURITY IN ELECTRONIC MEDICAL RECORDS

**BY**

**EDOSOMWAN, IMUETINYAN BOMA**
**(11CH012188)**
**B. Sc Management & Information System, Covenant University, Ota.**

**A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc) DEGREE IN MANAGEMENT AND INFORMATION SYSTEM IN THE DEPARTMENT OF COMPUTER AND INFORMATION SCIENCES, COLLEGE OF SCIENCE AND TECHNOLOGY, COVENANT UNIVERSITY, OTA, OGUN STATE, NIGERIA**

**OCTOBER, 2020**

# ACCEPTANCE

This is to attest that this dissertation was accepted in partial fulfilment of the requirements for the award of Master of Science (M.Sc.) degree in Management Information Systems in the Department of Computer and Information Science, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria.

**Miss. Adefunke F. Oyinloye**
**(Secretary, School of Postgraduate Studies)** **Signature and Date**

**Prof. Akan B. Williams**
**(Dean, School of Postgraduate Studies)** **Signature and Date**

# DECLARATION

I hereby declare that this dissertation entitled "**AN ENHANCED ATTRIBUTE-BASED PRETTY GOOD PRIVACY FILE ENCRYPTION FOR DATA SECURITY IN ELECTRONIC MEDICAL RECORDS"** was carried out by **EDOSOMWAN, IMUETINYAN BOMA** with matriculation number **11CH012188**. The project is centered on an original study in the Department of Computer and Information Sciences, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria, under the supervision of Prof. Victor Chukwudi Osamor. Concepts of this research project are the results of the research carried out by **EDOSOMWAN IMUETINYAN BOMA**, ideas of other researchers have also been fully recognized.

**EDOSOMWAN, IMUETINYAN BOMA**

**Signature and Date**

# CERTIFICATION

We certify that this dissertation titled "**AN ENHANCED ATTRIBUTE-BASED PRETTY GOOD PRIVACY FILE ENCRYPTION FOR DATA SECURITY IN ELECTRONIC MEDICAL RECORDS"** is an original work carried out by **EDOSOMWAN, IMUETINYAN BOMA (11CH012188)** in the Department of Computer and Information System, College of Science and Technology, Covenant University, Ota, Ogun State, Nigeria under the supervision of Prof. V.C. Osamor. We have examined and found this work acceptable as part of the requirements for the award of Master of Science in Management Information System.

**Prof. Victor C. Osamor**
**(Supervisor)** **Signature and Date**

**Prof. Olufunke O. Oladipupo**
**(Head of Department)** **Signature and Date**

**Prof. Olusegun Folorunsho**
**(External Examiner)** **Signature and Date**

**Prof. Akan B. Williams**
**(Dean, School of Postgraduate Studies)** **Signature and Date**

# DEDICATION

I dedicate this dissertation to my Heavenly Father-the source of all wisdom, strength and knowledge. I also dedicate it to my parents Mr. and Mrs. Bola Edosomwan and my siblings.

# ACKNOWLEDGEMENT

First and foremost, I want to thank God Almighty for his grace to start and complete this programme successfully. Secondly, my appreciation goes out to my wonderful parents Mr. and Mrs. Bola Edosomwan and my siblings for their unflinching support physically, financially, spiritually and morally from the beginning to the successful completion of the programme.

My sincere gratitude goes to the Chancellor of Covenant University, Dr. David Oyedepo, for receiving the vision and mission of Covenant University that has today become a reality, and to the entire Management of Covenant University for seeing that the vision has been fulfilled towards accomplishing great excellence through the master's academic programme.

I am very grateful to my supervisor, Prof Victor Chukwudi Osamor, for his patience, support, guidance and supervision throughout my master's programme. I also, want to appreciate him for being a father to me throughout the course of my programme.

I also appreciate the Head of Department of Computer and Information Sciences (CIS), Prof. Ambrose A. Azeta, the PG Coordinator, and the entire faculty members for their productive remarks during the numerous presentations we had during the cause of this work.

Finally, my appreciation goes to my wonderful friends in no particular order; Guembe Blessing, Koyejo Ooreofe, Omoremi Olushola Austin, Ani Osinachi Sylvester, Toro-Abasi Williams, Okezie Fiona, Agono Frank, Bishung Janet, Okezie Chidinma, who worked with me continuously to make this work a reality, and my colleagues for making the journey an enjoyable one despite the challenges we faced throughout the programme.

God richly and abundantly bless you all.

# TABLE OF CONTENTS

**CONTENT** **PAGE**

**COVER PAGE** **i**
**TITLE PAGE** **ii**
**ACCEPTANCE** **iii**
**DECLARATION** **iv**
**CERTIFICATION** **v**
**DEDICATION** **vi**
**ACKNOWLEDGEMENT** **vii**
**TABLE OF CONTENT** **viii**
**LIST OF FIGURES** **ix**
**LIST OF TABLES** **x**
**ABSTRACT** **xi**

**CHAPTER ONE:** **1**
**INTRODUCTION** **1**
1.1 Background Information **1**
1.2 Statement Of The Problem **6**
**1.3** Aim And Objectives Of The Study **8**
**1.4** Research Methodology **8**
**1.5** Significance Of The Study **10**
**1.6** Scope Of The Study **10**
1.7 Contribution To Knowledge **10**
1.8 Organisation Of The Dissertation **10**

**CHAPTER TWO** **12**
**LITERATURE REVIEW** **12**
2.1 Medical Records **12**
2.1.1 Significance Of Medical Records **15**
2.1.2 Challenges Affecting Medical Records **16**
2.2 Health Information System **17**
2.3 Electronic Medical Records (Emr) **18**
2.3.1 Emr Benefits, Drawbacks And Implementation Challenges **18**
2.3.2 Electronic Medical Record In Africa **20**
2.3.3 Electronic Medical Record In Nigeria **22**
2.4 The Concept Of Cryptography **24**
2.4.1 History Of Cryptography **27**
2.4.2 Various Cryptographic Algorithms **27**
2.4.2.1 Data Encryption Algorithm (Des) 30
2.4.2.2 Triple Data Encryption Algorithm (3des) 30
2.4.2.3 Cast-128 31

2.4.2.4 Blowfish 31
2.4.2.4 International Data Encryption Algorithm (Idea) 32
2.4.2.5 Advanced Encryption Standard (Aes) 32
2.4.2.6 Rc6 32
2.4.2.7 Rivest-Shamir-Adleman (Rsa) 33
2.4.3 Benefits And Drawbacks Of Cryptography **36**
2.5.4 Cryptography Application Areas **37**
2.4.5 The Concept Of Pretty Good Privacy **37**
2.4.6 Applications Of Pretty Good Privacy **39**
2.5 Mobile Devices **39**
2.5.1 Mobile Device Penetration In Nigeria **40**
2.6 Related Works **42**

**CHAPTER THREE** **45**
**RESEARCH METHODOLOGY** **45**
3.1 Overview Of The Current And Proposed System **46**
3.2 Adapted Framework **47**
3.3 Proposed Framework **48**
3.4 System Architecture **50**
3.5 Rivest-Shamir-Adleman Key Generation Algorithm **51**
3.6 File Decryption Authentication Pseudo Code **53**
3.7 Algorithm Implemented In The Emr **54**
3.8 Identification Of The Requirement Specification And Implementation Tools **60**
3.8.1 Functional Requirements **60**
3.8.2 Non-Functional Requirements **62**
3.8.3 Implementation Tools 62
3.8.3.1 Programming Languages 62
3.8.3.2 Patients’ Database 63
3.8.3.3 Doctors’ Database 63
3.8.4 System Requirement 63
3.8.4.1 Hardware Requirement 63
3.8.4.2 Software Requirement 63
3.9 Mapping Of Requirements To System Modules 63
3.10 System Requirement Modelling 65
3.10.1 Logical view 66
3.10.2 Implementation view 66
3.10.3 Deployment view 66
3.10.4 Process view 66
3.10.5 Use case view 67
3.11 System Modelling Diagrams 67

3.11.1 Use Case Diagram 67

3.11.2 Activity Diagram 68

3.11.3 Class Diagram 69

3.11.4 Component Diagram 70

3.11.5 Deployment Diagram 71

3.11.6 Sequence Diagram 72

3.11.7 State Diagram 74

3.12 Data Modelling 75

**CHAPTER FOUR 77**

**RESULTS 77**

4.1 Results Gathered From Initial Field Survey 77

4.2 Analysis Of Results From Semi-Structured Interview 90

4.3 Screenshots Of The Proposed Prototype System 92

4.4 Implementation tools 99

4.4.1 Netbeans Integrated Development Environment 99

4.4.2 Programming Language 99

4.4.3 Xampp 100

4.4.4 The Database Management System 100

4.5 System Usability Evaluation Using Iso 25010 Usability Model **100**

4.5.1 Survey Results Collected From Users 108

**CHAPTER FIVE 115**

**DISCUSSION 115**

5.1 Iso 25010 Usability Evaluation 115

5.2 Discussion 115

5.3 Observations Made During Research 123

**CHAPTER SIX 125**

**CONCLUSIONS AND RECOMMENDATIONS 125**

6.1 Summary 125

6.2 Conclusion 125

6.3 Contribution To Knowledge 126

6.4 Recommendations And Future Work 127

**REFERENCES 128**

**APPENDIX A 136**

**SYSTEM EVALUATION QUESTIONNAIRE 136**

**APPENDIX B 139**

**JAVA CODE FOR FILE SELECTION, ENCRYPTION AND DECRYPTION 139**

# LIST OF FIGURES

FIGURES LIST OF FIGURES PAGES

Figure 2.1: Challenges to the implementation of EMRS in Nigerian general hospitals 20

Figure 2.2: Diagram of the healthcare delivery system in Nigeria 23

Figure 2.3: Basic cryptography diagram 25

Figure 2.4: Single key or symmetric cryptography 26

Figure 2.5: Public key cryptography 27

Figure 2.6: Classification of cryptographic algorithm 30

Figure 2.7: Cryptographic algorithms key size (bits) 36

Figure 2.8: The working of PGP encryption technique 38

Figure 2.9: PGP encryption and decryption process 38

Figure 2.10: Mobile device penetration in Nigeria 40

Figure 2.11: Unique mobile users in Nigeria 41

Figure 2.12: Most mobilized country 41

Figure 3.1: Workflow of the methodology 45

Figure 3.2: Schema of the proposed system 47

Figure 3.3: Adapted framework 48

Figure 3.4: Proposed framework of the electronic medical record system 50

Figure 3.5: System architecture of the electronic medical record system 51

Figure 3.6: File decryption authentication 54

Figure 3.7: 4+1 architectural view model 66

Figure 3.8: Use case diagram for the electronic medical record system 67

Figure 3.9: Activity diagram for the electronic medical record system 68

Figure 3.10: Class diagram for the electronic medical record system 69

Figure 3.11: Component diagram of the electronic medical record system 70

Figure 3.12: Deployment diagram for the electronic medical record system 71

Figure 3.1: Sequence diagram for the EMRS the doctor's perspective 72

Figure 3.14 Sequence diagram for the EMRS the patient's perspective 73

Figure 3.15 State diagram for the electronic medical record system 74

Figure 4.1: Pie chart of presence of electronic medical record system 90

Figure 4.2: Pie chart of frequency of use of electronic medical record system 91

Figure 4.3: Screenshots of the doctor/admin login page 92

Figure 4.4: Screenshots of the patient login page 92

Figure 4.5: Screenshots of the doctor/admin registration page 93

Figure 4.6: Screenshots of the doctor/admin update page 94

Figure 4.7: Screenshots of the patient registration page 94

Figure 4.8: Screenshots of the patient registration page showing the full list of patients 95

Figure 4.9: Screenshots of the patient management page 95

Figure 4.10: Screenshots of the patient medical record page 96

Figure 4.11: Screenshots of the patient medical record page 96

Figure 4.12: Screenshots of the patient medical record page 97

Figure 4.1: Screenshots of the patient medical record page 97

Figure 4.14: Screenshots of the encryption and decryption pages 98

Figure 4.15: Screenshots of the encryption and decryption pages 98

Figure 4.1: ISO 25010 model 101

Figure 4.17: Pie chart of years of operation 104

Figure 4.18: Pie chart of patient size distribution 104

Figure 4.1: Pie chart of EMR awareness 105

Figure 4.20: Pie chart of EMR current usage 105

Figure 4.21: Pie chart of cryptography awareness 106

Figure 4.22: Pie chart of previous use of cryptographic enabled EMR 106

Figure 4.23: Bar chart of the functional suitability results 108

Figure 4.2: Bar chart of performance efficiency results 109

Figure 4.25: Bar chart of the compatibility results 109

Figure 4.26: Bar chart of the usability results 110

Figure 4.2: Bar chart of the reliability results 110

Figure 4.28: Bar chart of the security results 111

Figure 4.29: Bar chart of the maintainability results 111

Figure 4.30: Bar chart of the portability results 112

Figure 5.1: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for functional suitability 116

Figure 5.2: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for performance efficiency 117

Figure 5.3: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for compatibility 118

Figure 5.4: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for usability 119

Figure 5.5: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for reliability 120

Figure 5.6: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for security 121

Figure 5.7: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for maintainability 122

Figure 5.8: Bar chart of comparison in numeric ratio between the positive, neutral and negative feedback for portability 123

# LIST OF TABLES

**TABLES** **LIST OF TABLES** **PAGES**

Table 1.1: Comparison Of Cryptographic Algorithms On Various Parameters 5

Table 1.2: Tabular Mapping Between The Research Objectives And The Research Methodology 9

Table 2.1: Selected Open Source Electronic Medical Record Systems Available In Africa 21

Table 2.2: Electronic medical record implementation in some African countries 22

Table 2.3: Implementation of open MRS in some Nigerian hospitals 24

Table 2.4: An atbash cipher 28

Table 2.5: A skytale cipher 28

Table 2.6: The Polybius square 29

Table 2.7: The Ceasar cipher 29

Table 2.8: Comparison of cryptographic algorithms based on various parameters 35

Table 3.1: Hardware requirements 63

Table 3.2: Requirements and description 63-64

Table 3.3: Module and requirements 65

Table 3.4: Doctors table 74

Table 3.5: Patients table 75

Table 4.1: Semi- structured interview questions 76

Table 4.2: Result of the hospital digitization level 77-88

Table 4.3: Statistics of presence of electronic medical record systems 89

Table 4.4: Statistics of frequency of use of electronic medical record systems 91

Table 4.5: Statistics of hospitals personal data 102

Table 4.6: Statistic result for personal data of hospitals 107

Table 4.7: A summary of the result from the questionnaire 107

Table 4.8: Usability evaluation results collected from users 112-114

# ABSTRACT

Whenever an individual uses a service, registers for email, completes a financial transaction or goes to a doctor, Some level of personal information has to be provided. The fact remains that whether or not you are aware specific data and information about you is captured and stored by both government and non-governmental agencies. Citizens have to develop a level of trust in both government and other sectors that the data they provide is secure and will be kept confidential. Hence, it is the role of these agencies to adopt data protection practices that will limit or completely eliminate data exploitation, manipulation and theft. The health sector in Nigeria continues to be a victim of data theft or mismanagement of patient medical data and this is credited to the poor and terrible way personal data are managed including poor medical record management system. Over the years there have been reoccurring cases of missing medical records or mismanaged record keeping in healthcare organizations which often leads to legal actions against such healthcare organizations or use of patient data for malicious intent. In order to overcome this, the patient record system must be protected to thwart off multiple duplicitous behaviours and ensure confidentiality and reliability. Cryptography presents various methods and cryptographic algorithms to ensure security in file transfer and secure record management. Thus, the aim of this study is to propose a cryptographic enabled Electronic Medical Record system that utilizes the concept of random key generation. The study investigated 50 hospital and primary health care centres in Alimosho Local Government Area of Lagos State to assess the level of digitalization of medical records which directly impacts on data privacy and security. The proposed system is evaluated using the ISO 25010 usability model which analyses eight (8) various constructs which are functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability and portability. Based on these constructs, a questionnaire will be designed and distributed for hospital review on the proposed system and the results will be analysed with the help of SPSS software. It was discovered that large number of hospitals and primary healthcare centres are not digitize raising great concerns on the implementation of data security in treatment centres. The overall results should show that the proposed system has a good usability rating which ultimately implies that it can be utilized in a healthcare organization for safe record management and secure file transfer and future recommendation for EMR as Cloud-native application.

**Keywords: Electronic Medical Records (EMR), Cryptography, Cloud Computing, Pretty Good Privacy encryption technique, Data privacy**.